IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF INDIANA
SOUTH BEND DIVISION

ASPEN AMERICAN INSURANCE COMPANY, as Subrogee of Trinity Health Corporation, and TRINITY HEALTH CORPORATION	)	Civil Action No. 3:22-CV-0044-JD-MGG
Plaintiffs,	)	**FIRST AMENDED COMPLAINT**
v.	)	**JURY DEMANDED**
BLACKBAUD, INC.,	)	
Defendant.	)	

AMENDED COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiffs, ASPEN AMERICAN INSURANCE COMPANY ("Aspen"), as subrogee of Trinity Health Corporation, and TRINITY HEALTH CORPORATION ("Trinity Health"), by and through their respective undersigned counsel, and, for causes of action against Defendant BLACKBAUD, INC. ("Defendant" or "Blackbaud"), hereby allege as follows:

Nature of the Action

1. From February 7, 2020 to May 20, 2020, Blackbaud experienced a ransomware incident that infected its computer systems (the "Incident") causing damages to Plaintiffs.

2. Defendant touts itself as a world leading software company and application service provider ("ASP") that non-profits rely on to secure highly-sensitive information, including personal information from donors and patients.

3. Trinity Health is an Indiana not-for-profit corporation with a multi-facility health system, including the Saint Joseph Health System that serves St. Joseph County, Indiana and other counties across northern Indiana and twenty-two other states across the nation.

4. During in-person meetings between Trinity Health and Blackbaud in 2015, Blackbaud made representations concerning its services, practices, and ability to secure highly-sensitive information, which Trinity Health relied upon in deciding whether to engage Blackbaud's services.

5. Blackbaud's services included maintaining servers containing Trinity Health's data, including patients' and donors' protected health information ("PHI") and names, addresses, and other information ("PII") that was proprietary to Trinity Health ("Confidential Information") (collectively, "Trinity Data").

6. Blackbaud's verbal and written representations to Trinity Health during pre-contract discussions concerning its services, practices, and ability to secure highly-sensitive information were demonstrably false.

7. Following Blackbaud's sales pitches, and in reliance upon the statements made by Blackbaud, on June 17, 2015, Trinity Health entered a Master ASP Services MSA (the "MSA") with Blackbaud, which governed Blackbaud's handling of Confidential Information.

8. Based on the same assurances, Trinity Health entered into a separate Business Associate Agreement ("BAA"), which governed Trinity Health's and Blackbaud's relationship as a Covered Entity and Business Associate under Health Insurance Portability and Accountability Act ("HIPAA") and the Health Information Technology for Economic and Clinical Health ("HITECH") Act and Blackbaud's handling of PHI as Trinity Health's agent.

9. On February 7, 2020, a third party was able to readily bypass Blackbaud's substandard security and penetrate Blackbaud's systems and deploy ransomware.

10. The Incident resulted in attackers gaining access to Trinity Data in Blackbaud's possession.

11. While Blackbaud had full access to insurance proceeds under its insurance policies, Trinity Health was deprived of access to those insurance proceeds because Blackbaud failed to name Trinity Health as an additional insured as required under the MSA.

12. Plaintiffs were damaged due to Blackbaud's breaches of the "Services," "Duty of Confidentiality," "Security," "Meaningful Use," "Limited Data Use," and "Industry and Security Standards" provisions of the MSA, among others.

13. Blackbaud failed to maintain adequate security, failed to timely notify Trinity Health of the Incident as required under the BAA and as Trinity Health's agent, and actively concealed information concerning the Incident from Trinity Health. Blackbaud's action meant that Trinity Health had to undertake its own investigation of the Incident in order to comply with applicable laws.

14. Blackbaud breached the BAA and its fiduciary duties by failing to comply with its obligations as a "business associate" under HIPAA, HITECH, and any implementing regulations, before, during and after the Incident. This meant that Trinity Health had to undertake its own investigation of the Incident in order to comply with applicable laws.

15. Trinity Health was required to comply with numerous state and federal statutes and regulations because of Blackbaud's misrepresentations, negligence, failures, and breaches.

16. Compliance with these various laws caused damages to Plaintiffs because Trinity Health was required to:

a. retain legal experts to assess and comply with Trinity Health's legal obligations to its patients and donors;

b. retain computer experts to investigate the data breach as required under law and expected by regulators;

c. retain firms to draft, translate, print, and mail letters required under data breach notification laws and expected by regulators;

d. maintain a call center to respond to patient and donor inquiries, as expected by regulators; and

e. provide credit monitoring for affected patients and donors, as required under various state laws and expected by federal regulators (collectively, "Remediation Damages").

17. Blackbaud used its insurance to cover its own identical remediation costs and the funds from that policy should have been made available to Trinity Health as an additional insured.

18. Blackbaud's failure to name Trinity Health as an additional insured under its own insurance policy resulted in Plaintiffs having to shoulder the burden of the Remediation Damages.

19. In addition, Trinity Health had to implement new data retention protocols and build a new process to handle patients and donors opting-out from future contact.

20. Plaintiffs' damages total an amount no less than $2,317,432.39, plus interest, and continue to accrue because of the ongoing fallout of the Incident.

The Parties

21. Aspen is a corporation organized in Texas and its principal place of business is located in Rocky Hill, CT.

22. Trinity Health is an Indiana not-for-profit corporation with a multi-facility health system, including the Saint Joseph Health System that serves St. Joseph County, Indiana and other counties across northern Indiana twenty-two other states across the nation.

23. Blackbaud is a Delaware corporation with its principal place of business in Charleston, South Carolina and has been continuously doing business in the State of Indiana. Blackbaud's

common stock is publicly traded on the NASDAQ under the ticker symbol "BLKB." Blackbaud may be served with process through its Registered Agent for service of process, Corporation Service Company, 135 North Pennsylvania Street, Suite 1610, Indianapolis, IN, 46204.

Jurisdiction and Venue

24. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(a)(1) because it is a civil action between citizens of Indiana and Delaware, and the matter in controversy exceeds the sum or value of $75,000, exclusive of interest and costs.

25. Venue is proper in this Court under 28 U.S.C. § 1441(a), which expressly provides that the proper venue of a removed action is "the district court of the United States for the district and division embracing the place where such action is pending." The Northern District of Indiana, South Bend Division is the district embracing St. Joseph County, Indiana, the place where this action was originally pending before being removed to this Court. 28 U.S.C. 94(a)(2).

Statement of Facts

a. *Blackbaud's False Representations*

26. Prior to entering into the MSA or BAA, representatives of Trinity Health attended sales meetings with representatives of Blackbaud. During Blackbaud's sales meetings, its representatives corresponded with, gave presentations to, and provided written materials to Trinity Health's representatives.

27. Blackbaud's correspondence made representations concerning Blackbaud's data security. Those documents made representations concerning Blackbaud's ability to keep data entrusted to it secure. Trinity Health relied on these statements when entering into the MSA and BAA, but they were false.

28. Despite Blackbaud's representations that it provided robust cybersecurity services, its security program was woefully inadequate. Blackbaud's unsound, vulnerable systems containing valuable data were an open invitation for a months-long intrusion and exfiltration by cybercriminals.

b. *The MSA*

29. Based on representations made by Blackbaud, Trinity Health entered into a service agreement for Blackbaud's software and subscription ASP services. [1] On June 17, 2015, Trinity Health entered the MSA with Blackbaud to provide services that consolidated existing databases into one system of records across Trinity Health for enhanced constituent management. A true, complete, and accurate copy of the MSA is attached as Exhibit A.

30. In the MSA, Blackbaud represented itself as a provider of ASP services and professional services for nonprofit organizations and made representations and warranties and undertook obligations thereunder.[2]

31. Under the MSA, Blackbaud also agreed to perform ASP services and its other obligations under the MSA "in a manner that complies with all applicable federal, state and local laws, rules, regulations and standards" and "shall take all measures to promptly remedy any violation(s) of Applicable Law in the performance of the Services and its obligations under [the] MSA, and shall promptly notify Trinity of any violation(s) thereof."[3]

---

[1] MSA, § 4.

[2] MSA, § 5.1 "Services"; § 7.1 "Duty of Confidentiality"; § 7.5 "Security"; § 8.6 "Meaningful Use"; § 9.4 "Limited Data Use": and § 3(a) "Industry and Security Standards" provisions of the MSA, among others.

[3] MSA, § 8.1 "General Compliance."

32. Blackbaud's services under the MSA included maintaining servers containing Trinity Data, including Trinity Health's Confidential Information.[4]

33. Moreover, Blackbaud was required to add Trinity Health as an additional insured.[5]

34. Blackbaud breached the MSA by failing to comply with industry and regulatory standards by neglecting to implement security measures to mitigate the risk of unauthorized access, utilizing outdated servers, storing obsolete data, and maintaining unencrypted data fields.

35. Upon information and belief, on February 7, 2020, a third party was able to readily bypass Blackbaud's substandard security and penetrate Blackbaud's systems and deploy ransomware.

36. Blackbaud further breached the MSA by failing to add Trinity Health as an additional insured, depriving Trinity Health of access to $50 million of insurance proceeds that should have been available to reimburse Trinity Health for its damages that arose from the ransomware attack.

c. *The BAA*

37. The MSA does not create a Covered Entity-Business Associate relationship.

38. Therefore, the MSA states that the BAA will be executed and that the BAA governs and controls Blackbaud's handling of PHI.[6] Any terms concerning an agency relationship in the MSA are inconsequential to whether an agency relationship existed between Trinity Health and Blackbaud in regard to Blackbaud's handling of PHI as a Business Associate under the BAA.[7]

39. Blackbaud and Trinity Health entered into a BAA, effective June 17, 2015. A copy of the BAA is attached as Exhibit C.

---

[4] MSA, § 1, "Confidential Information" & "Trinity Health Data"; § 7.1 "Duty of Confidentiality".

[5] MSA, § 10.

[6] MSA § 7.6.

[7] MSA § 7.6.

40. Under the BAA, Blackbaud was responsible for handling PHI, and, therefore, Blackbaud was Trinity Health's agent in its capacity as a Business Associate. In addition, Trinity Health was entitled to give interim instructions and directions to Blackbaud regarding PHI. Specifically, the BAA requires Trinity Health's authorization and approval for Blackbaud's transfer, handling, and storage of PHI.[8]

41. During the process of assimilating Trinity Health's data, which included PHI and PII from millions of individuals, including Trinity Health patients, donors, and affiliates, Blackbaud and Trinity Health worked together to build a custom database. The database included numerous fields such as the individuals name, address, and other information that would be considered PHI or PII. The database also included a "notes" field that allowed for the capture of unique information of individuals on an "as needed" basis. The database also allowed Trinity Health to upload attachments related to individuals.

42. As a hospital and healthcare provider, Trinity Health must comply with HIPAA and the HITECH Act, including the U.S. Department of Health and Human Services ("HHS") implementing regulations.

43. Under such regulations, "[a] health care provider who transmits any health information in electronic form" is a "Covered Entity." 45 CFR § 160.103, Covered Entity, (3).

44. Under the same regulations, a "Business Associate" includes a corporation who (i) "[o]n behalf of such covered entity or of an organized health care arrangement . . . in which the covered entity participates, . . . creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety

[8] BAA §§ F.4, H.5, M.2 & N.

activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing;" or (ii) "[p]rovides . . . , legal, actuarial, accounting, consulting, data aggregation . . . , management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person." 45 CFR § 160.103, Business Associate, (1)(i)-(ii).

45. In addition, a "Business Associate" includes "[a] Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information." 45 CFR § 160.103, Business Associate, (3)(i).

46. A 2013 HIPAA amendment made it easier for HIPAA Covered Entities, such as Trinity Health, to identify patients for donations by using software solutions like those offered by Blackbaud to enrich electronic Protected Health Information ("ePHI") to maximize outreach to wealthy patients capable of making a meaningful philanthropic gift to the hospital.

47. ePHI is PHI that is produced, saved, transferred, or received in electronic form. PHI is "[i]ndividually identifiable health information . . . received by a health care provider, health plan, employer or healthcare clearing house [and its Business Associates] . . . [that] [r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual . . . [t]hat identifies the individual; or [w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. §§ 160.103, *et seq.*

48. HIPAA/HITECH mandated security specifications are risk-driven and certain measures must be taken if, after a risk assessment, the specified security measure is determined to be "reasonable and appropriate" in the risk management of the confidentiality, availability, and integrity of ePHI.

49. HIPAA and its implementing regulations, 45 C.F.R. §§ 160, *et seq.*, establish privacy and security standards for certain health organizations and their "business associates." *See id.* § 164.302.

50. Covered Entities and their Business Associates, which process PHI and ePHI, must meet strict privacy and security standards propounded by HHS pursuant to HIPAA and HITECH. HHS's Office for Civil Rights ("OCR") is responsible for enforcing the Privacy and Security Rules under HIPAA and HITECH.

51. Blackbaud is a Business Associate, as that term is defined in HIPAA and HITECH, providing functions that involve the use or disclosure of PHI by Covered Entities, like Trinity Health. As a Business Associate, Blackbaud is directly subject to the HIPAA Security Rule.

52. Blackbaud is a "business associate" subject to HIPAA because it receives, maintains, or transmits its customers' PHI. *Id.* § 160.103. "PHI" includes, in relevant part, individually identifiable health information relating to the provision of health care. *Id.*

53. Under the BAA, Blackbaud represented to Trinity and agreed to comply with the forgoing obligations as a "business associate" under HIPAA, HITECH, and any implementing regulations.[9]

54. Blackbaud agreed "to implement reasonable administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of all PHI." [10]

[9] BAA, § B.

[10] BAA, § G.1.

55. Blackbaud agreed "to implement reasonable electronic security practices for [Trinity Health's] PHI which is transmitted, stored, collected, created, received, maintained, or used in electronic form" and "to encrypt PHI transmitted by [Blackbaud] to [Trinity Health] over a public network"[11]

56. Blackbaud was required to report any "actual or suspected privacy incident, breach of security, intrusion or unauthorized use or disclosure of PHI or ePHI" within ten business days.[12]

57. HIPAA required Blackbaud to ensure the confidentiality of the electronic PHI it received and maintained by protecting against reasonably anticipated threats to its integrity. *Id.* § 160.306(a). To do so, Blackbaud was required to implement reasonable and appropriate security measures to mitigate the risk of unauthorized access to its customers' electronic personal health information, including by encrypting certain data where appropriate. *See id.* §§ 164.308 (administrative safeguards), 164.312 (technical safeguards).

58. Blackbaud was aware of the significant privacy and security obligations of Covered Entities and their Business Associates mandated by HIPAA and HITECH and the Privacy and Security Rules.

59. Blackbaud understood both the value and the risk of using ePHI for fundraising purposes. As stated in one of its white papers, Blackbaud understood:

> [t]he new HIPAA rules offer great opportunity for hospitals and health systems to reach out in a more meaningful way to the individuals and families who have the greatest affinity to them — their patients. **However, with this opportunity comes great responsibility to establish business processes that allow for successful fundraising but also manage and protect the patient data entrusted to you**.[13]

---

[11] BAA, § G.1.

[12] BAA, § G.2.

[13] Susan U. McLaughlin, Blackbaud, *HIPAA, PHI, and You* 4 (Feb. 2015), https://www.blackbaud.com/files/resources/downloads/2015/02.15.HIPAA_GratefulPatient.Whitepaper.pdf (emphasis added).

60. Blackbaud breached its obligations as a "business associate" under the BAA by failing to comply with HIPAA, HITECH, and implementing regulations.

61. As a Business Associate, Blackbaud is directly liable for HIPAA violations for any "failure to comply with the requirements of the Security Rule."

62. As a Business Associate, Blackbaud is also directly liable for HIPAA violations for any "failure to provide breach notification to a covered entity or another business associate."

63. The HIPAA Breach Notification Rule, 45 C.F.R. § 164.400-414, requires HIPAA Covered Entities and their Business Associates to provide notification following a breach of unsecured PHI. Similar breach notification provisions implemented and enforced by the FTC, apply to vendors of personal health records and their third-party service providers, pursuant to Section 13407 of the HITECH Act.

64. A HIPAA breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the PHI. An impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment.

65. Where there is an unauthorized disclosure or ransomware attack on PHI the Business Associate must document by "thorough and accurate evaluation the evidence acquired and analyzed" to determine whether there is a "low probability of compromise."[14]

[14] Off. for C.R., U.S. Dep't Health Hum. Servs., *FACT SHEET: Ransomware and HIPAA* 6 (2016), https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.

66. Blackbaud breached the BAA and its fiduciary duties as Trinity Health's agent by failing to comply with its obligations as a "business associate" under HIPAA, HITECH, and any implementing regulations

d. *Common Law Duty*

67. Trinity Data included Confidential Information such as patient and donor names, addresses, and other information that is proprietary to Trinity Health.

68. Blackbaud was in a superior position to safeguard Trinity Health's Confidential Information, therefore, Blackbaud also owed a duty to Trinity Health to comply with statutes, regulations, and industry standards in safeguarding Confidential Information.

69. Blackbaud breached that common law duty by failing to heed warning signs that Trinity Health's Confidential Information could be stolen.

e. *The Incident*

70. Upon information and belief, Blackbaud maintained Trinity Data on a shared network, server, and/or software. Despite its own awareness of steady increases of cyberattacks on health care providers over the course of recent years, Blackbaud did not maintain adequate security of Trinity Data and did not adequately protect it against hackers and cyberattacks.

71. Upon information and belief, Blackbaud maintained Trinity Data on servers that were obsolete.

72. Upon information and belief, the servers were not on the system patch schedule and were "forgotten machines."

73. Upon information and belief, Blackbaud had planned on upgrading the old servers to new technology.

74. Upon information and belief, the servers that were breached included data from an older Trinity Health database called "Raiser's Edge", which included information from 575,638 Trinity Health constituents (i.e., patients, donors, and affiliates).

75. Upon information and belief, the servers that were breached also included data from an older Trinity Health database called "eTapestry", which included information from numerous Trinity Health constituents (i.e., patients, donors, and affiliates).

76. Upon information and belief, the older servers were operating multiple applications, and Blackbaud wanted to eventually merge them onto a new, base application on one server.

77. Upon information and belief, upgrading to new technology had been "on a laundry list for a while."

78. Upon information and belief, employees at Blackbaud became increasingly alarmed with Blackbaud's failure to patch old systems, and even eventually emailed executives about the vulnerabilities—receiving a response from one executive: "we're working on it."

79. Upon information and belief, a former information security analyst warned Blackbaud about process vulnerabilities that would subject them to attack—such as using remote desktop access and the vulnerabilities that had been uncovered in security scans.

80. Upon information and belief, the remote desktop access configuration was particularly concerning for a year leading up to the Incident — so much so that s/he or his/her team member would simply "shut down the machines" because they knew the risk was too high to allow them to continue to operate.

81. Upon information and belief, prior to the Incident a former information security analyst advised that CrowdStrike needed to be installed on Blackbaud's machines to capture logs, including the logs that were later erased by the ransomware in this case.

82. Upon Information and belief, a bad actor compromised Blackbaud's networks starting February 2020. Blackbaud's servers were compromised, and data exfiltration occurred. This data was then encrypted by the bad actor.

83. Upon information and belief, Blackbaud did not discover the ransomware until on or around May 14, 2020.

84. Upon information and belief, because Blackbaud elected not to install a program on their servers that would have assisted in the forensic investigation of the Incident, the data that would normally be used in a forensic investigation is limited.

85. Upon information and belief, the aforementioned analyst's team suggested a year prior to the Incident that the data on Blackbaud's servers needed to be encrypted to reduce vulnerabilities; however, because the servers were so old, the "exact nature of the data was unknown."

86. Upon information and belief, the Incident was the result of Blackbaud's failure not only to properly and adequately determine whether it was susceptible to a data breach but also its negligent and reckless failure to remove old unused and obsolete data containing Trinity Data or to encrypt such information.

87. Upon information and belief, Blackbaud's retention of this Trinity Data in unencrypted form on older legacy versions of its programs made public exposure of such data in a cyberattack very likely.

88. Upon information and belief, there was no valid business reason to continue to maintain this information on its systems.

89. The failure was knowing, reckless and, at bare minimum, negligent given the known risks to Blackbaud—particularly given vendor announcements regarding the sunset of certain databases and Blackbaud's failure to move Trinity Data to newer systems with more robust security features.

90. As a result of Blackbaud's lax data protection standards, cybercriminals obtained access not only to recently-obtained information, but Trinity Data that remained on backup files for years, if not decades.

91. The Incident resulted in attackers gaining access to Trinity Data in Blackbaud's possession.

92. Had Blackbaud maintained a sufficient security program, including properly monitoring its network, security, and communications, it would have discovered the cyberattack sooner or prevented it altogether.

93. Upon information and belief, the ransomware attack that began in February 2020 and continued until May 2020 was twofold: the cybercriminals copied data from the systems and held it for ransom, and upon being discovered, the cybercriminals attempted but allegedly failed to block Blackbaud from accessing its own systems.

94. Upon information and belief, the ransomware attack led to the removal of one or more copies of some or all of the accessed data.

95. Upon information and belief, once removed, the hackers could easily have re-copied the stolen data.

96. Upon information and belief, on May 14, 2020, Blackbaud retained Kudelski Security to "investigate unauthorized activity and scripts detected throughout" Blackbaud's systems.

97. Upon information and belief, Kudelski Security completed its analysis on June 10, 2020, and issued the report ("the Report") on July 14, 2020,[15] two days before Blackbaud contacted Trinity Health to inform it about the Incident.

[15] Kudelski Security, Blackbaud Incident Report (July 14, 2020).

98. Upon information and belief, the Report shows that Blackbaud did not have a sufficient security program in place to prevent cyberattack and access, and to address the full scope of the Incident.

99. Upon information and belief, the Report highlights the steps it could have taken—but failed to take—to prevent the Incident.

100. In sum, Blackbaud failed to maintain its information on current databases—it failed to heed vendor announcements regarding the sunset of certain databases, leaving client information, including Trinity Health, on older databases that were more vulnerable to cyberattack.

101. Based on the foregoing, Blackbaud made false misrepresentations, breached its contractual obligations to Trinity Health under the MSA and BAA, breached its fiduciary obligations as Trinity Health's agent, and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard Blackbaud's computer systems and the data it maintained. Blackbaud's wrongful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security program to reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect Trinity Data;

c. Failing to properly monitor its own data security programs for existing intrusions;

d. Failing to destroy highly confidential personal data information including Social Security numbers on its legacy software which was unnecessarily kept on Blackbaud's systems despite no reasonable or practicable business reason for doing so;

e. Misrepresenting the extent to which Trinity Data was exposed by the breach;

f. Misrepresenting that Blackbaud would maintain reasonable security measures;

g. Concealing that Blackbaud did not adopt reasonable security measures; and

h. Failing to timely notify Trinity Health of the data breach.

102. As the result of Blackbaud's failure to take certain measures to prevent the attack before it occurred, Blackbaud negligently and wrongfully failed to safeguard Trinity Data.

103. Blackbaud did not inform Trinity Health of the Incident until July 16, 2020.

104. In correspondence dated July 16, 2020, Blackbaud advised Trinity Health that "our Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking our system access and fully encrypting files; and ultimately expelled them from our system."

105. Blackbaud also advised Trinity Health that "[t]he cybercriminal did not access credit card information, bank account information, or social security numbers"… and further advised that "the cybercriminal did not gain access to bank account information, usernames, passwords, or social security numbers stored in your database because they were encrypted. None of your data was lost or corrupted as a result of this incident."

106. Blackbaud also advised Trinity Health that it had no reason to believe that any data went beyond the cybercriminal or that any data would be disseminated of other made available publicly.

107. Blackbaud further advised Trinity Health that it did not consider the security incident to be a reportable incident under HIPAA or US state breach notification laws but provided Trinity Health with a constituent toolkit in the event that Trinity Health came to a different conclusion. Blackbaud admitted that "[i]t is unlikely but possible, depending on jurisdiction, that our customers may have to make further notifications to constituents or other third parties…" and

advised Trinity Health "…to also consult with your organization's legal counsel to understand any notification requirements."

f. *Trinity Health Responds to the Incident*

108. After learning of the Incident, Trinity Health met with Blackbaud on July 24, 2020 and July 30, 2020 to obtain specific information related to the Trinity Health data involved in the security incident.

109. During these meetings, Blackbaud reported that their analysis did not include specific detail related to the level of compromise that would be needed to facilitate individual notifications. Blackbaud also declined to participate or assist with individual notifications.

110. During these meetings, Trinity Health also requested that Blackbaud provide a copy of the Trinity Health data involved in the incident. Blackbaud delivered the requested data to Trinity Health on August 6, 2020.

111. After receiving a copy of the data affected from Blackbaud, Trinity Health began reviewing the copy of the impacted data and determined that the attack included ransomware with exfiltration that impacted backup files maintained by Blackbaud, including Trinity Health's Philanthropy donor database ("Confidential Information," *supra*).

112. Trinity Health also determined that the impacted data included information from 2000 to 2020 and consisted of a customized module that included information such as donors relationships to patients, patient discharge status, patient insurance and patient department of service, patient name, contact information, and donation history. This information was not encrypted and could be read in clear text. Further, a limited number of individuals identified in the data above also had a Social Security number and/or financial account information listed in a field that was also not encrypted.

113. The unencrypted information above constitutes protected health information "PHI" under HIPAA.

114. During its review of the data associated with the breach, Trinity Health relied on a 2106 Guidance Document from HHS entitled "FACT SHEET: Ransomware and HIPAA" which indicates that "[a] breach under the HIPAA Rules is defined as, "…the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.402.6.

115. The Guidance Document also indicates that "[w]hen electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a 'disclosure' not permitted under the HIPAA Privacy Rule."

116. The Guidance Document also indicates that "[u]nless the covered entity or business associate can demonstrate that there is a '…low probability that the PHI has been compromised,' based on the factors set forth in the Breach Notification Rule, a breach of PHI is presumed to have occurred."

117. Relying on the above, Trinity Health determined that the ransomware attack at issue constituted a breach, as the bad actors had exfiltrated Trinity Health's data contained PHI from Blackbaud's servers, which the bad actors then encrypted prior to demanding a ransom.

118. Trinity Health also reviewed and considered the four factors discussed in the Guidance Document and identified in 45 CFR § 164.402(2), including "(i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification; (ii) The unauthorized person who used the protected health information or to

whom the disclosure was made; (iii) Whether the protected health information was actually acquired or viewed; and (iv) The extent to which the risk to the protected health information has been mitigated."

119. After reviewing these factors, and the extent of the compromised data, as set forth in paragraphs 111 and 112, Trinity Health could not determine that there was a low probability of actual compromise, and therefore determined the incident was a breach that required reporting.

120. Having determined that it had to report the breach, Trinity Health, with assistance from its attorneys and Kroll, a company specializing in cybersecurity and breach notification, determined that the data accessed during the incident contained unencrypted information regarding approximately 3,289,937 patients. Of those, 164 patients also had financial information exposed in the data breach. Identification of these individuals required considerable effort by Trinity Health, its attorneys, and Kroll.

121. Beginning on September 14, 2020, Trinity Health, through Kroll, began mailing "[w]ritten notification by first-class mail . . . at the last known address of the" 3,289,937 patients identified above and incurred significant printing and postage expenses associated with these notifications.[16]

122. Finally, since more than ten mailing addresses for the patients above were incorrect or "bad", per HIPAA requirements set forth in 45 CFR § 164.404(d)(2), Trinity Health posted substitute notice on its website beginning on August 2020, which was subsequently updated with HIPAA compliant content as the data analysis was completed. Trinity Health also issued notices to statewide media in all 50 states via PR Newswire on September 14, 2020 in accordance with its

[16] 45 CFR § 164.404(d)(1) ("(i) **Written notification by first-class mail to the individual at the last known address of the individual** or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail." (emphasis added)).

duties under HIPAA to notify media in states or jurisdictions where it was notifying 500 or more residents. In addition, Trinity Health included a toll-free phone number for individual to learn whether their unsecured protected health information may be included in the breach.

123. Finally, based on State regulations Trinity Health notified individuals and state regulators in Colorado, Connecticut, Washington D.C., Illinois, Indiana, Louisiana, Massachusetts, Montana, New Hampshire, Vermont, and Virginia of the incident, as individuals from these states were identified in the breach data received from Blackbaud.

124. Trinity Health considered Colorado Revised Statute 6-1-716 which defines a "security breach" as an "unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a covered entity" and mandates that "a covered entity that maintains, owns, or licenses computerized data that includes personal information about a resident of Colorado shall, when it becomes aware that a security breach may have occurred, . . . the covered entity shall give notice to the affected Colorado residents." C.R.S. 6-1-716 (2)(a). The statute also sets forth the notice requirements. Pursuant to the mandates set forth in C.R.S. 6-1-716, Trinity Health determined that notification of Colorado residents and the Colorado Office of the Attorney General was required and therefore forwarded notifications to the Attorney General and 2,320 Colorado residents regarding the incident. (See Exhibit D).

125. Trinity Health also considered the Connecticut General Statutes Annotated which defines a "breach of security" as "unauthorized access to or unauthorized acquisition of electronic files, media, databases or computerized date, containing personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable." Conn. Gen. Stat. Ann. § 36a-

701b(a)(1). Further, "[a]ny person who owns, licenses or maintains computerized data that includes personal information, shall provide notice of any breach of security following the discovery of the breach to any resident of this state whose personal information was breached or is reasonably believed to have been breached." Conn. Gen. Stat. Ann. § 36a-701b(b)(1). If a notice of a breach of security is required by subdivision (1), "[t]he person who owns, licenses, or maintains computerized data that includes personal information, shall, not later than the time when notice is provided to the resident, also provide notice of the breach of security to the Attorney General." Conn. Gen. Stat. Ann. § 36a-701b(b)(2)(A). The statute continues to set forth the notice requirements. Pursuant to the mandates set forth in Conn. Gen. Stat. Ann. § 36a-701b, Trinity Health determined that notification of Connecticut Attorney General and Connecticut residents was required and therefore forwarded notifications to 863 Connecticut residents and the Office of the Connecticut Attorney General regarding the incident. (See Exhibit E).

126. Trinity Health also considered The District of Columbia Code which defines a "breach of the security of the system" as "unauthorized acquisition of computerized or other electronic data or any equipment or device storing such data that compromises the security, confidentiality, or integrity of personal information maintained by the person or entity who conducts business in the District of Columbia." D.C. Code Ann. § 28-3851(1)(A). "Any person or entity who conducts business in the District of Columbia, and who, in the course of such business, owns or licenses computerized or other electronic data that includes personal information, and who discovers a breach of the security of the system, shall promptly notify any District of Columbia resident whose personal information was included in the breach." D.C. Code Ann. § 28-3852(a). The statute continues to set forth the notice requirements. Pursuant to the mandates set forth in D.C. Code Ann. § 28-3852, Trinity Health determined that notification of the Attorney General

and District of Columbia residents was required and therefore forwarded notifications to the Office of the District of Columbia Attorney General and 8,644 residents regarding the incident. (See Exhibit F).

127. Trinity Health also considered the Illinois Compiled Statutes Annotated, which defines a "breach of the security of the system data" as an "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector." 815 ILCS 530/5. "Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach." 815 ILCS 530/10(a). The statute also sets forth the notice requirements. Pursuant to the mandates set forth in 815 ILCS 530/10, Trinity Health determined that notification of the Attorney General and Illinois residents was required and therefore forwarded notifications to the Office of the Illinois Attorney General and 310,601 Illinois residents regarding the incident. (See Exhibit G)

128. Trinity Health also considered the Indiana Code which defines a "breach of the security of data" as an "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person." Ind. Code Ann. § 24-4.9-2-2(a). "[A]fter discovering or being notified of a breach of the security of data, the data base owner shall disclose the breach to an Indiana resident whose: (1) unencrypted personal information was or may have been acquired by an unauthorized person; or (2) encrypted personal information was or may have been acquired by an unauthorized person with access to the encryption key; if the data base owner knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity

deception, identity theft, or fraud affecting the Indiana resident." Ind. Code Ann. § 24-4.9-3-1(a).The statute continues to set forth the notice requirements. Pursuant to the mandates set forth in Ind. Code Ann. § 24-4.9-3-1, Trinity Health determined that notification of Attorney General and 67 Indiana residents was required and therefore forwarded notifications as required by this incident. (See Exhibit H)

129. Trinity Health also considered the Louisiana Revised Statutes which define a "breach of the security of the system" as "the compromise of the security, confidentiality, or integrity of computerized data that results in, or there is a reasonable likelihood to result in, the unauthorized acquisition of and access to personal information maintained by an agency or person." La. Stat. Ann. § 51:3073(2). Any person that owns, licenses, or maintains "computerized data that includes personal information that the agency or person does not own shall notify the owner or licensee of the information if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person through a breach of security of the system containing such data, following discovery by the agency or person of a breach of security of the system." La. Stat. Ann. § 51:3074(C),(D). The statute also sets forth notice requirements. Pursuant to the mandates set forth, Trinity Health determined that notification of the Louisiana Department of Justice and 2 Louisiana residents was required, and therefore forwarded notifications. (See Exhibit I).

130. Trinity Health also considered the Massachusetts General Laws which define a "breach of security" as "the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth."

Mass. Gen. Laws ch. 93H, §1. "A person or agency that owns or licenses data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the attorney general, the director of consumer affairs and business regulation and to such resident, in accordance with this chapter." Mass. Gen. Laws ch. 93H, §3(b). The statute continues to set forth the notice requirements. Pursuant to the Massachusetts statutory requirements, Trinity Health determined that notification of the Massachusetts Office of the Attorney General and 293 Massachusetts residents was required and therefore forwarded notifications to Massachusetts residents regarding this incident. (See Exhibit J).

131. Trinity Health also considered the Montana Code Annotated which states that "[a]ny person or business that conducts business in Montana and that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the data system following discovery or notification of the breach to any resident of Montana whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person." Mont. Code Ann. § 30-14-1704(1). The statute continues to set forth the notice requirements. Pursuant to the Montana Code, Trinity Health determined that notification of the Montana Department of Justice and 4 Montana residents was required and therefore forwarded notifications. (See Exhibit K).

132. Trinity Health also considered the New Hampshire Revised Statutes, which define a "security breach" as an "unauthorized acquisition of computerized data that compromises the security or confidentiality of personal information maintained by a person doing business in this

state. Good faith acquisition of personal information by an employee or agent of a person for the purposes of the person's business shall not be considered a security breach, provided that the personal information is not used or subject to further unauthorized disclosure." N.H. Rev. Stat. § 359-C:19(V). The statute also indicates that "[a]ny person doing business in this state who owns or licenses computerized data that includes personal information shall, when it becomes aware of a security breach, promptly determine the likelihood that the information has been or will be misused. If the determination is that misuse of the information has occurred or is reasonably likely to occur, or if a determination cannot be made, the person shall notify the affected individuals as soon as possible as required under this subdivision." N.H. Rev. Stat. § 359-C:20(I)(a). The statute continues to set forth notice requirements. Pursuant to the New Hampshire statutes, Trinity Health determined that notification of the Consumer Protection Bureau of the Office of the New Hampshire Attorney General and 9 New Hampshire residents was required and therefore forwarded notifications regarding this incident. (See Exhibit L).

133. Trinity Health also considered the Annotated Vermont Statutes, which define a "security breach" as an "unauthorized acquisition of electronic data, or a reasonable belief of an unauthorized acquisition of electronic data, that compromises the security, confidentiality, or integrity of a consumer's personally identifiable information or login credentials maintained by a data collector." Vt. Stat. Ann. Tit. 9, § 2430(13)(A). And "[a]ny data collector that owns or licenses computerized personally identifiable information or login credentials shall notify the consumer that there has been a security breach following discovery or notification to the data collector of the breach." Vt. Stat. Ann. tit. 9, § 2435(b)(1). The statute continues to set forth notice requirements. Pursuant to the mandates set forth, Trinity Health determined that notification of the Office of the

Attorney General and 932 Vermont residents was required and therefore forwarded notifications regarding this incident. (See Exhibit M).

134. Trinity Health also considered the Annotated Code of Virginia, which defines a "breach of the security of the system" as "the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused, or will cause, identity theft or other fraud to any resident of the Commonwealth." Va. Code Ann. § 18.2-186.6(A). Further, "[i]f unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and causes, or the individual or entity reasonably believes has caused or will cause, identity theft or another fraud to any resident of the Commonwealth, an individual or entity that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to the Office of the Attorney General and any affected resident of the Commonwealth without unreasonable delay." Va. Code Ann. § 18.2-186.6(B). The statute continues to set forth notice requirements. Pursuant to the mandates set forth, Trinity Health determined that notification of Office of the Virginia Attorney General and 20 Virginia residents was required and therefore forwarded notifications this incident. (See Exhibit N).

135. Upon information and belief, all the recipients of the written notice by mail in the foregoing states did not qualify for notice by electronic mail.

136. Trinity Health also reviewed various state statutes, and determined that Connecticut law requires its impacted residents be offered access to credit monitoring services for at least 24

months when the security of a resident's name and Social Security number has been compromised; Massachusetts law requires its impacted residents be offered access to credit monitoring services for a period of at least 18 months when the security of a resident's name and Social Security number has been compromised; and, Washington, D.C. law requires its impacted residents be offered access to credit monitoring services for a period of not less than 18 months when the security of a resident's Social Security number or taxpayer identification number has been compromised. *See* Conn. Gen. Stat. Ann. § 36a-701b(b)(2)(B); Mass. Gen. Laws Ann. Ch. Ch. 93H, § 3A(a); D.C. Code Ann. § 28-385.02.

137. Trinity Health also reviewed, considered its duty to mitigate any harmful effect of disclosure of PHI, and exercised its judgment in offering credit monitoring to potentially affected individuals in response. 45 C.F.R. § 164.530(f). To that end, HSS believes "that allowing flexibility and judgment by those familiar with the circumstances to dictate the approach is the best approach to mitigating harm." Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462, 82748 (Dec. 28, 2000).

138. OCR expects credit monitoring services to be one of several means used to mitigate any harm to patients as a result of exposing their PHI, if "those familiar with the circumstances" determine such credit monitoring services are "the best approach to mitigating harm." 65 Fed. Reg. 82462, 82748 (Dec. 28, 2000).

139. Blackbaud's initial and continuing breaches forced Trinity Health to retain legal counsel and computer experts to investigate the incident, evaluate the data as set forth above, determine that breach notification was required, notify impacted patients and donors, set up credit

monitoring and an information call center, and comply with applicable laws and the expectations of regulators ("Remediation Damages", *supra*).[17]

140. Plaintiffs incurred legal costs to investigate the Incident, advise Trinity Health on its compliance obligations under the law following the Incident, draft notice letters required under various laws, and communicate with States' Attorneys General and other regulators.

141. Trinity Health was legally obligated to investigate the Incident.

142. Trinity Health was obligated under the laws of the states of where potentially affected individuals resided to provide them with written notice.

143. Trinity Health incurred costs to translate notice letters into the languages spoken by the potentially affected individuals in order to provide the legally required notice.

144. Plaintiffs incurred costs for computer experts to investigate the root cause of the Incident, identify the data that was potentially exposed, and identify the individuals whose PII or ePHI was potentially exposed.

145. Plaintiffs incurred costs for printing and mailing the legally required notice letters to potentially affected individuals concerning the Incident.

146. Plaintiffs incurred costs for an information call center to provide information to Trinity Health's patients and donors that were potentially affected by the Incident.

147. Plaintiffs incurred costs for credit monitoring as required under the laws of the states of Connecticut, Massachusetts, the District of Columbia, 45 C.F.R. § 164.530(f), and as expected by regulators, including states' Attorneys General and the Office of Civil Rights.

[17] *Trinity Health's Response to the Blackbaud Philanthropy Database Security Incident* (Sept. 14, 2020), https://www.prnewswire.com/news-releases/trinity-healths-response-to-the-blackbaud-philanthropy-database-security-incident-301130466.html.

148. In addition, Trinity Health had to implement new data retention protocols and build a new process to handle patients and donors opting-out from future contact.

g. *Blackbaud's Failure to Add Trinity Health as an Additional Insured*

149. Blackbaud used its insurance to cover its own identical remediation costs and the funds from its policy should have been made available to Trinity Health as an additional insured pursuant to the MSA.

150. Blackbaud's failure to name Trinity Health as an additional insured under its own insurance policy deprived Trinity Health of access to $50 million of insurance proceeds that should have been available to reimburse Trinity Health to cover these Remediation Damages.

h. *Aspen*

151. Trinity Health is an Aspen insured under an Aspen APEX Cyber Insurance Policy ("the Policy"). A redacted copy of the Policy is attached as Exhibit B.

152. As Trinity Health's insurer, and in accordance with the terms of the Policy, Trinity Health paid amounts covered under the retention for Remediation Damages incurred because of the Incident, including, but not limited to, credit monitoring services and call centers, legal counsel, computer systems recovery, and data recovery and data migration services (*i.e.*, the Remediation Damages).

153. Under the Policy Aspen issued to Trinity Health, Trinity Health was responsible to pay the retention and Aspen paid covered amounts in excess of the Policy's retention up to the limit of liability, a combined total of over $2.3 million paid by Trinity Health and Aspen to date.

154. The Policy Aspen issued to Trinity Health grants Aspen the right to pursue third parties, like Blackbaud, for the amounts paid by Trinity Health in satisfaction of the retention and by Aspen under the Policy. The Policy contains a subrogation clause that states as follows:

> H. Subrogation. If any payment is made under this Policy for Loss or Expense, and there is the ability to recover against any third party, it is agreed that the Insured tenders all its rights of recovery to the Insurer. The Insured also agrees to assist the Insurer in exercising such rights. Any recovery will first be paid to the Insurer toward any incurred subrogation expenses, Loss or Expense, and any remaining amounts will be paid to the Insured for reimbursement of any Retention paid.

155. The subrogation clause grants Aspen the right to recover from Blackbaud the Remediation Damages paid by Trinity Health in satisfaction of the retention and the Remediation Damages paid by Aspen under the Policy. Aspen seeks to recover from Blackbaud the damages suffered by Trinity Health and Aspen because of the Incident.

COUNT I
NEGLIGENT MISREPRESENTATION

156. Plaintiffs re-allege and incorporate each of the foregoing allegations of this Complaint with the same force and effect as if fully set forth herein.

157. Trinity Health entered into discussions with Blackbaud with the expectation that Blackbaud would encrypt and maintain Trinity Data on a shared network, server, and/or software because of Blackbaud's reputation as a provider of ASP Services that non-profits rely on to secure highly-sensitive information, including personal information from donors and patients, and so Trinity Health could consolidate existing databases into one system of records across Trinity Health for enhanced constituent management.

158. The MSA and BAA made clear, among other things, Blackbaud's obligations as a "business associate" under HIPAA, HITECH, and any implementing regulations.[18]

159. The nature of the services to be provided created a public interest in seeing that Blackbaud could ascertain with reasonable care whether its representations of its services were accurate. Instead, Blackbaud made misrepresentations that it could, among other things, comply

[18] BAA, § B.

with such federal law and regulations as well as industry standards to maintain reasonable and appropriate physical, administrative, and technical measures to keep Trinity Data confidential and to protect it from unauthorized access and disclosure.

160. In doing so, Blackbaud failed to ascertain whether such representations were accurate.

161. Trinity Health placed confidence in Blackbaud's misrepresentations based on its reputation as a purported world leading software company and Trinity Health's reliance on such misrepresentations was an inducement for executing the MSA and BAA with Blackbaud.

162. As a direct and proximate result of Blackbaud's negligent misrepresentation, Trinity Health was required to comply with numerous state and federal statutes and regulations.

163. Compliance with these various laws required Trinity Health to retain legal experts to assess and comply with its legal obligations to its patients and donors; retain computer experts to investigate the data breach as required under law and expected by regulators; retain firms to draft, translate, print, and mail letters required under data breach notification laws and expected by regulators; maintain a call center to respond to patient and donor inquiries, required under data breach notification laws and as expected by regulators; and provide credit monitoring for affected patients and donors, as required under various state laws and expected by federal regulators.

164. As a result, Trinity Health, and its subrogee Aspen, suffered damages.

165. The damages suffered by Trinity Health, and its subrogee Aspen, include, but are not limited to, paying the Remediation Damages.

166. These damages total an amount no less than $2,317,432.39, and continue to accrue because of the ongoing fallout of the Incident.

COUNT II
BREACH OF THE MSA

167. Plaintiffs re-allege and incorporate each of the foregoing allegations of this Complaint with the same force and effect as if fully set forth herein.

168. The MSA between Blackbaud and Trinity Health is valid and enforceable.

169. Blackbaud had duties under the MSA to, among other things, protect Trinity Data, including encrypting Trinity Data; properly and adequately determine whether Blackbaud was susceptible to a data breach properly; maintain and monitor its own data security programs for intrusions; and, remove old unused and obsolete data containing Trinity Data or to encrypt such information.

170. Under the MSA, Blackbaud agreed not to disseminate Trinity Data[19] and not to copy, reproduce or transfer any Confidential Information.[20]

171. Under the MSA, Blackbaud agreed to carry and maintain Commercial General Liability insurance and Network liability insurance naming Trinity as an additional insured under its policies. [21]

172. Blackbaud breached its duties under the MSA by, among other things, failing to adequately protect Trinity Data; failing to properly and adequately determine whether Blackbaud was susceptible to a data breach; failing to properly maintain and monitor its own data security programs for intrusions; failing to remove old unused and obsolete data containing Trinity Data or to encrypt such information; failing to heed vendor announcements regarding the sunset of certain

[19] MSA § 9.4.

[20] MSA § 7.1.

[21] MSA, § 10.

databases, leaving client information on older databases that were more vulnerable to cyberattack; and, failing to name Trinity Health as an additional insured under its policies.

173. Blackbaud also breached its duties by disseminating Trinity Data to third parties and permitting them to copy, reproduce and transfer such Confidential Information.

174. As a direct and proximate result of Blackbaud's breaches of the MSA, Trinity Health was required to comply with numerous state and federal statutes and regulations.

175. Compliance with these various laws required Trinity Health to retain legal experts to assess and comply with its legal obligations to its patients and donors; retain computer experts to investigate the data breach as required under law and expected by regulators; retain firms to draft, translate, print, and mail letters required under data breach notification laws and expected by regulators; maintain a call center to respond to patient and donor inquiries, required under data breach notification laws and as expected by regulators; and provide credit monitoring for affected patients and donors, as required under various state laws and expected by federal regulators.

176. As a direct and proximate result of Blackbaud's breaches of the MSA by permitting third parties to copy, reproduce and transfer Trinity Health's Confidential Information, Trinity Health's good will was injured and it had to implement new data retention protocols and build a new process to handle patients and donors opting-out from future contact.

177. As a direct and proximate result of Blackbaud's breaches of the MSA by failing to name Trinity Health as an additional insured under Blackbaud's own insurance policy, Trinity Health was deprived of access to $50 million of insurance proceeds that should have been available to reimburse Trinity Health to cover these Remediation Damages.

178. Instead, Trinity Health was required to turn to its insurer, Aspen, to cover its costs in order to be in compliance with numerous state and federal statutes and regulations.

179. As a result of these breaches, Trinity Health, and its subrogee Aspen, suffered damages.

180. The damages suffered by Trinity Health, and its subrogee Aspen, include, but are not limited to, paying the Remediation Damages.

181. These damages total an amount no less than $2,317,432.39, and continue to accrue because of the ongoing fallout of the Incident.

COUNT III
BREACH OF THE BAA

182. Plaintiffs re-allege and incorporate each of the foregoing allegations of this Complaint with the same force and effect as if fully set forth herein.

183. The BAA between Blackbaud and Trinity Health is valid and enforceable.

184. Blackbaud had duties under the BAA to, among other things, protect PHI, including encrypting PHI; properly and adequately determine whether Blackbaud was susceptible to a data breach properly; maintain and monitor its own data security programs for intrusions; and, remove old unused and obsolete data containing or to encrypt such information.

185. Under the BAA, Blackbaud agreed to comply with its obligations as a "business associate" under HIPAA, HITECH, and any implementing regulations.[22]

186. In addition, Blackbaud was required under the BAA to report any "actual or suspected privacy incident, breach of security, intrusion or unauthorized use or disclosure of PHI or ePHI" within ten business days. [23]

187. Blackbaud breached its duties under the BAA by, among other things, failing to adequately protect consumers' PHI; failing to properly and adequately determine whether

[22] BAA, § B.

[23] BAA, § G.2.

Blackbaud was susceptible to a data breach; failing to properly maintain and monitor its own data security programs for intrusions; failing to remove old unused and obsolete data containing PHI or to encrypt such information; and, failing to heed vendor announcements regarding the sunset of certain databases, leaving client information on older databases that were more vulnerable to cyberattack.

188. Blackbaud also breached its duties by disseminating Trinity Data to third parties and permitting them to copy, reproduce and transfer such PHI.

189. In addition, Blackbaud breached its duties under the BAA by failing to comply with its obligations as a "business associate" under HIPAA, HITECH, and any implementing regulations.[24]

190. Finally, Blackbaud further breached its duties under the BAA by, among other things, failing to inform Trinity Health of the Incident within ten business days of knowing the "actual or suspected" Incident was occurring on May 14, 2020.[25] Instead, Blackbaud notified Trinity Health of the Incident on July 16, 2020, forty-two (42) days after it "suspected" and had knowledge of the "actual" Incident.

191. As a direct and proximate result of Blackbaud's breaches of the BAA, Trinity Health was required to comply with numerous state and federal statutes and regulations.

192. Compliance with these various laws required Trinity Health to retain legal experts to assess and comply with its legal obligations to its patients and donors; retain computer experts to investigate the data breach as required under law and expected by regulators; retain firms to draft, translate, print, and mail letters required under data breach notification laws and expected

[24] BAA, § B.

[25] BAA, § G.2.

by regulators; maintain a call center to respond to patient and donor inquiries, required under data breach notification laws and as expected by regulators; and provide credit monitoring for affected patients and donors, as required under various state laws and expected by federal regulators.

193. As a result, Trinity Health, and its subrogee Aspen, suffered damages.

194. The damages suffered by Trinity Health, and its subrogee Aspen, include, but are not limited to, paying the Remediation Damages.

195. These damages total an amount no less than $2,317,432.39, and continue to accrue because of the ongoing fallout of the Incident.

COUNT IV
NEGLIGENCE

196. Plaintiffs re-allege and incorporate each of the foregoing allegations of this Complaint with the same force and effect as if fully set forth herein.

197. Blackbaud was in a superior position to safeguard Trinity Health's Confidential Information, therefore, Blackbaud owed a duty to safeguard/protect Trinity Health's Confidential Information.

198. Blackbaud breached that common law duty by ignoring warning signs that Trinity Health's Confidential Information could be stolen.

199. As a direct and proximate result of Blackbaud's negligence, Trinity Health was required to comply with numerous state and federal statutes and regulations.

200. Compliance with these various laws required Trinity Health to retain legal experts to assess and comply with its legal obligations to its patients and donors; retain computer experts to investigate the data breach as required under law and expected by regulators; retain firms to draft, translate, print, and mail letters required under data breach notification laws and expected by regulators; maintain a call center to respond to patient and donor inquiries, required under data

breach notification laws and as expected by regulators; and provide credit monitoring for affected patients and donors, as required under various state laws and expected by federal regulators.

201. As a result, Trinity Health, and its subrogee Aspen, suffered damages.

202. The damages suffered by Trinity Health, and its subrogee Aspen, include, but are not limited to, paying the Remediation Damages.

203. These damages total an amount no less than $2,317,432.39, and continue to accrue because of the ongoing fallout from the Incident.

COUNT V
GROSS NEGLIGENCE

204. Plaintiffs re-allege and incorporate each of the foregoing allegations of this Complaint with the same force and effect as if fully set forth herein.

205. Blackbaud was in a superior position to safeguard Trinity Health's Confidential Information, therefore, Blackbaud owed a duty to safeguard/protect Trinity Health's Confidential Information.

206. Blackbaud intentionally breached that common law duty in reckless disregard of the consequences because it was previously warned about process vulnerabilities that would subject it to attack and stored Trinity Health's Confidential Information on obsolete servers.

207. As a direct and proximate result of Blackbaud's gross negligence, Trinity Health was required to comply with numerous state and federal statutes and regulations.

208. Compliance with these various laws required Trinity Health to retain legal experts to assess and comply with its legal obligations to its patients and donors; retain computer experts to investigate the data breach as required under law and expected by regulators; retain firms to draft, translate, print, and mail letters required under data breach notification laws and expected by regulators; maintain a call center to respond to patient and donor inquiries, required under data

breach notification laws and as expected by regulators; and provide credit monitoring for affected patients and donors, as required under various state laws and expected by federal regulators.

209. As a result, Trinity Health, and its subrogee Aspen, suffered damages.

210. The damages suffered by Trinity Health, and its subrogee Aspen, include, but are not limited to, paying the Remediation Damages.

211. These damages total an amount no less than $2,317,432.39, and continue to accrue because of the ongoing fallout of the Incident.

COUNT VI
BREACH OF FIDUCIARY DUTY (WITH RESPECT TO PHI)

212. Plaintiffs re-allege and incorporate each of the foregoing allegations of this Complaint with the same force and effect as if fully set forth herein.

213. Blackbaud acted for the benefit of Trinity Health by maintaining Trinity Data on Blackbaud's shared network, server, and/or software in a fiduciary capacity as Trinity Health's agent in its handling of PHI as a Business Associate.

214. Trinity Health relied on Blackbaud's promise to maintain reasonable and appropriate physical, administrative, and technical measures to keep PHI confidential and to protect it from unauthorized access and disclosure.

215. Blackbaud breached its fiduciary duties in acting on behalf of Trinity Health by, among other things, failing to adequately protect consumers' PHI; failing to properly and adequately determine whether Blackbaud was susceptible to a data breach; failing to properly maintain and monitor its own data security programs for intrusions; failing to remove old unused and obsolete data containing PHI or to encrypt such information; and, failing to heed vendor announcements regarding the sunset of certain databases, leaving client information on older databases that were more vulnerable to cyberattack.

216. Under the BAA, Blackbaud was also required to report any "actual or suspected privacy incident, breach of security, intrusion or unauthorized use or disclosure of PHI or ePHI" within ten business days.[26]

217. Specifically, Blackbaud was required to report "the identification of each individual whose PHI or ePHI has been, or is reasonably believed . . . to have been accessed, acquired, or disclosed in connection with an actual or suspected breach of privacy, security, or HITECH." [27]

218. Blackbaud was also required to provide "any other available information" that Trinity Health "is required under HIPAA to include in a notification to an individual." [28]

219. Blackbaud breached its fiduciary duties by failing to disclose the "actual or suspected" Incident for at least two months after learning about it.[29]

220. Blackbaud breached its fiduciary duties by presenting Trinity Heath with inaccurate information about the Incident.

221. Blackbaud breached its fiduciary duties by failing to cooperate with Trinity Health's investigation and improperly withheld information that was critical to Trinity Health.

222. In the absence of meaningful information from Blackbaud, under 45 C.F.R. § 164.530(f), Trinity Health was required to assess the Incident on its own and effectuate its compliance with applicable regulations.

223. As a direct and proximate result of Blackbaud's breach of fiduciary duty, Trinity Health was required to comply with numerous state and federal statutes and regulations.

[26] BAA § G.2 (emphasis added).

[27] BAA § G.3.

[28] BAA § G.3.

[29] BAA § G.2.

224. Compliance with these various laws required Trinity Health to retain legal experts to assess and comply with its legal obligations to its patients and donors; retain computer experts to investigate the data breach as required under law and expected by regulators; retain firms to draft, translate, print, and mail letters required under data breach notification laws and expected by regulators; maintain a call center to respond to patient and donor inquiries, required under data breach notification laws and as expected by regulators; and provide credit monitoring for affected patients and donors, as required under various state laws and expected by federal regulators.

225. The damages suffered by Plaintiffs, include, but are not limited to, paying the Remediation Damages.

226. These damages total an amount no less than $2,317,432.39, plus interest, and continue to accrue because of the ongoing fallout of the Incident.

227. Irrespective of whether Blackbaud's breach of fiduciary duty caused these damages, Blackbaud can be required to disgorge all compensation received while breaching its fiduciary duties.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully prays that this Court enter judgment in its favor and grant the following relief:

a. declaring Defendant made negligent misrepresentations to Trinity Health and awarding Plaintiffs damages in an amount no less than $2,317,432.39 plus interest;

b. declaring Defendant in breach of the MSA and awarding Plaintiffs damages in an amount no less than $2,317,432.39 plus interest, and all other reasonable and appropriate damages that would flow from Blackbaud's breach of the MSA;

c. declaring Defendant in breach of the BAA and awarding Plaintiffs damages in an amount no less than $2,317,432.39 plus interest, and all other reasonable and appropriate damages that would flow from Blackbaud's breach of the BAA;

d. declaring Plaintiffs' damages to be caused by Defendant's negligence and awarding Plaintiffs damages in an amount no less than $2,317,432.39 plus interest;

e. declaring Plaintiffs' damages to be caused by Defendant's gross negligence and awarding Plaintiffs damages in an amount no less than $2,317,432.39 plus interest, and all other reasonable and appropriate damages that would flow from Blackbaud's gross negligence;

f. declaring Defendant to have breached its fiduciary duty to Trinity Health and awarding Plaintiffs damages in an amount no less than $2,317,432.39 plus interest, and all other reasonable and appropriate damages that would flow from Blackbaud's breach of fiduciary duty;

g. awarding Plaintiffs punitive damages for the Counts asserted, as appropriate;

h. awarding Plaintiffs all costs and expenses of this action, including reasonable attorneys' fees; and

i. awarding Plaintiffs such further relief as the Court may deem just, necessary, and proper.

REQUEST FOR TRIAL BY JURY

Plaintiffs respectfully request trial by jury on all issues so triable.

Dated: September 28, 2022

/s/Kirk D. Bagrowski
Kirk D. Bagrowski, 23495-53
Eichhorn & Eichhorn, LLP
2929 Carlson Drive, Suite 100
Hammond, IN 46323
(219) 931-0560
kbagrowski@eichhorn-law.com

/s/ Robert J. Feldt
Robert J. Feldt, 16311-45
Eichhorn & Eichhorn, LLP
2929 Carlson Drive, Suite 100
Hammond, IN 46323
(219) 931-0560
rfeldt@eichhorn-law.com

Attorneys for Plaintiff
TRINITY HEALTH CORPORATION

/s/ Michael A. Kreppein
Michael A. Kreppein, 22430-64
WILSON, ELSER, MOSKOWITZ,
EDELMAN & DICKER LLP
233 E. 84th Drive – Park Tower, Suite 201
Merrillville, IN 46410
Telephone: (219) 525-0560
Michael.Kreppein@wilsonelser.com

/s/ Marc S. Voses
Marc S. Voses, Esq.
(MV-8869, *pro hac vice* to be filed)
CLYDE & CO US LLP
405 Lexington Ave., 16th Floor
New York, NY 10174
(212) 710-3968
marc.voses@clydeco.us

Attorneys for Plaintiff
ASPEN AMERICAN INSURANCE COMPANY

CERTIFICATE OF SERVICE

I, Kirk D. Bagrowski, hereby certify that on the 28th day of September 2022, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which sent notification of such filing to the following:

James M. Lewis
Michael J. Hays
TUESLEY HALL KONOPA, LLP
212 East LaSalle Avenue, Suite 100
South Bend, IN 46617

Richard S. Glaser
Jason R. Benton
Corri A. Hopkins
Sarah F. Hutchins
PARKER POE ADAMS & BERNSTEIN, LLP
620 S Tryon St Ste 800
Charlotte, NC 28202

Michael A. Kreppein
WILSON, ELSER, MOSKOWITZ,
EDELMAN & DICKER LLP
233 E. 84th Drive - Park Tower, Suite 201
Merrillville, IN 46410

/s/Kirk D. Bagrowski
Kirk D. Bagrowski